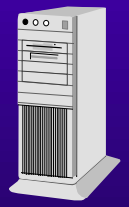
DMS/Medium Grade Services ‘GO Configure’

Doug Colligan, Litton/PRC
Kevin Heald, SRA International
MGS Lab (703) 824-4624

Medium Grade Services Definition

DMS/MGS is secure interoperable commercial off-the-shelf (COTS) email that uses the DOD Public Key Infrastructure (PKI) Medium Assurance certificates for signature and encryption



Configured COTS

+

DoD PKI Certificate

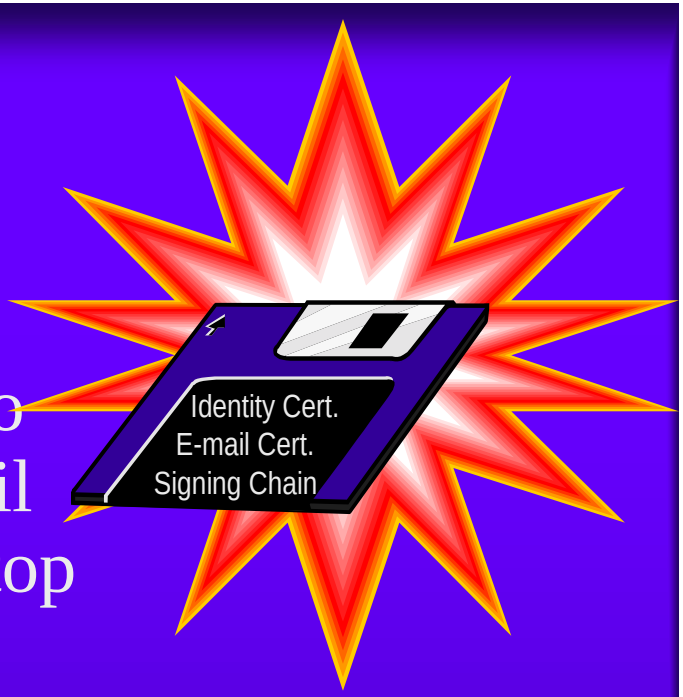
=

Secure COTS Email

High Grade DMS vs MGS

Mail Application	Certificate Level	Mail/Protocol	Classification
High Grade DMS	Class 4 - Fortezza	Organizational - X.400	SBU/ Confidential + above
Medium Grade Services (MGS)	Class 3	Individual - SMTP	SBU

Background



- MGS allows DOD PKI registered user's the ability to digitally sign & encrypt email messages with existing desktop email software.
- DOD PKI Registered users are issued Key pairs. 3 Files to install on users' workstations

User A → User B

Sign Message
Sign with A's Private Key

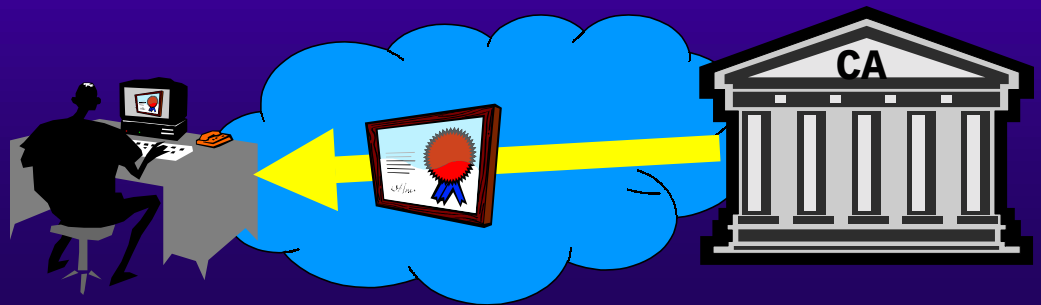
Sign Message
Validate with A's Public key

Encrypt Message
Encrypt with B's Public Key

Encrypt Message
Decrypt with B's Private Key

Supporting PKI Registration

- Obtaining certificates for MGS requires a PKI registration process - C/S/A designates Local Registration Authorities (LRAs).
- LRA uses a special configured workstation to register users:
  - Win NT 4 SP 3 +
  - Netscape Navigator 4.7 w/Personal Security Module (PSM)
  - Dedicated Printer
- Once LRA Registers users, PKI user retrieves certificates using a "kiosk" workstation using Netscape Navigator 4.7 w/PSM
- (MS Internet Explorer not permitted to retrieve certificates)



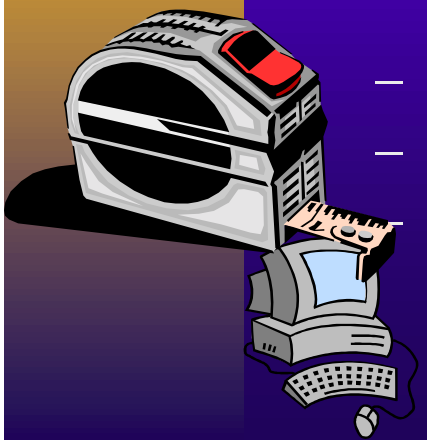
Microsoft Requirements:
(Exchange Server DMS or 5.5 SP 2+)

Windows 9x Client:

- Minimum
  - Windows 95
  - IE 5 128 Bit Security
  - Outlook 98 and/or DMS 2.1
- Optimum
  - Windows 98 2nd Edition
  - IE 5.01 128 Bit Security
  - Outlook 2000 SR-1

Windows NT Client

- Minimum
  - NT 4 SP4 (128 Bit)
  - IE 4.01
  - Outlook 98 and/or DMS 2.1
- Optimum
  - Windows 2000 Professional
  - IE 5.01
  - Outlook 2000 SR-1



Lotus Notes Requirements:
(Notes Server 5.01a+)

- Win 9x or NT Operating System
- Notes 5.01a client or higher

Netscape Requirements:
(Notes Server or Exchange Server)

- Win 9x or NT Operating System
- Netscape Messenger 4.6 +

COTS Facts of Life

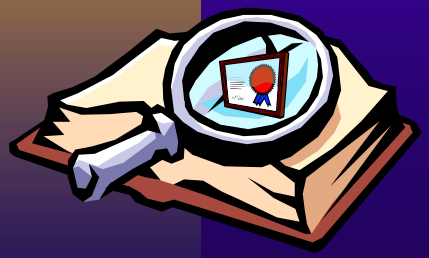
- New product releases and versions occur frequently
- COTS versions generally newer than fielded DMS User Agents
- Configuration is Everything!
  - A wide variety of configurations will work for basic SMTP
  - Only a few configurations will work for MGS
  - Pilot sites often have heterogeneous configurations installed

Client Upgrade

- Vendor products are becoming more S/MIME compatible in every release.
  - Outlook 97 - Not S/MIME compatible
  - Notes 5.0 or lower - Not compatible with DOD PKI
- Microsoft Outlook 2000 adds functionality & fixes bugs.
- Free Client Upgrades: If you have the Exchange Client Access License it is a FREE upgrade to Outlook 2000 (and SR-1).

Public Key Distribution

- In order for user to encrypt messages to a recipient, the sender must have the user's public key.
- Key can be obtained from (DEMO):
  - Signed message and stored in a user's contact's list
  - Download Key from DOD PKI web site:
    - http://ds-2-ent.den.disa.mil/ds/search
  - Use Public Key stored in a MS Exchange GAL
    - http://ds-1-ent.chamb.disa.mil/ds/search



Local Directory Challenge

- Problem: Storing certificates in Exchange Contact Lists creates maintenance problems (CRLs, Expiration)
- Near Term Solutions:
  - Install CertPub on Exchange Server to allow users to publish and retrieve their public keys
  - Install a Directory Product (Netscape) and combine registration data with DEERS/Rapids Unique ID to populate directory
- Long Term Solution: Use DMS or Global Information Grid Directory

MGS Tools

- CertPub: Visual Basic application run on an Exchange Server that publishes users public keys the GAL. (DEMO)
- InstallCert: is a executable script that automates the process of configuring workstation to be MGS enabled. (DEMO)

MGS/PKI Interoperability Summit 24-25 Apr 00

- Joint Service Participation
- Top 5 Issues
  - Configuration PKI Issues
  - Functionality of a Client with PKI
  - Client Interoperability
  - Certificate Distribution
- Vendor Participation - Microsoft/Netscape
- http://falcon3.ncr.disa.mil

MGS Bottom Line

- MGS is PKI Ready and being used today
  - *PKI Ready* is Changing
- MGS Team is *jump starting* PKI implementation
- Email crosses all boundaries and is on every desktop
- The time is right for MGS implementation
- Continue work with vendors, develop tools, test products & processes, and manage knowledge for the benefit of all DOD users

MGS is not a *product* - it is a *capability*

The
ENEMY
is listening

He wants to know
what you know

KEEP IT TO YOURSELF

Deploy Secure COTS E-mail